RESOLUTION ON INFORMATION TECHNOLOGY MONITORING

WHEREAS, in 2017, the Virginia Tech Board of Visitors evaluated its committee structure, realigned their responsibilities, and created two new committees. Specifically, the Board of Visitors created the Compliance, Audit, and Risk Committee to provide oversight of enterprise risk management, and the Governance and Administration Committee to oversee administrative functions, including information technology; and

WHEREAS, cyberattacks seeking to obtain sensitive data and disrupt mission-critical activities at institutions of higher education have become more prevalent, posing an elevated risk to students, faculty, and staff at the university; and

WHEREAS, Virginia Tech is committed to supporting all members of the university community in conducting research, coursework, and business in a technologically secure environment; and

WHEREAS, for the past several years, the Board of Visitors' committees have been monitoring the cyber risks confronting Virginia Tech and meeting with university leadership to evaluate best practices and consider what measures should be taken to mitigate risk to the university and those individuals who could be impacted by threats to its information technology infrastructure, data, and other IT assets; and

WHEREAS, the Board of Visitors recognizes the importance of balancing the university's business needs and respect for its members' freedom of expression and inquiry; yet changes in digital technologies demonstrate the need to update effective governance processes to protect the university digital assets and actions; and

WHEREAS, the routine security monitoring of information technology networks, electronic communications and data stored on technology resources or in the cloud has been adopted as a best practice by governmental agencies, private-sector industry, and other higher education institutions;

NOW, THEREFORE, BE IT RESOLVED that to mitigate the elevated risk to the university and those individuals who potentially could be impacted by threats to its information technology infrastructure, data and other IT assets, the Virginia Tech Board of Visitors directs the leadership of the university to enhance monitoring of electronic communications and records whether stored on university technology resources, in the university's cloud storage, or in transit on the university network, consistent with the Commonwealth of Virginia's policy that "no user should have any expectation of privacy in any message, file, image or data created, sent, retrieved, or received by use of the Commonwealth's equipment and/or access"; and

BE IT FURTHER RESOLVED that the university will revise all relevant policies as quickly as possible to ensure transparency and full disclosure of IT-automated routine monitoring for security and risk mitigation purposes and will make it clear that access to equipment and data will occur only for legitimate business or IT security compliance purposes and will be limited to the minimum degree necessary to accomplish the specified cybersecurity-related purpose; and,

LASTLY, BE IT RESOLVED that the Board of Visitors delegates authority henceforth to the Executive Vice President and Chief Operating Officer (or designee) to revise any existing university policies and standards, such as policies 7010, 7035, and 7105, or create new policies and standards as necessary to mitigate the risks described herein.

RECOMMENDATION:
That the resolution directing that governance processes, tools, and continuous monitoring as described within the resolution of all university communications networks and forms of electronic communications and records whether stored on university technology resources, in the university's cloud storage, or in transit on the university network be implemented as quickly as feasible, that all relevant policies and standards be revised accordingly, and that authority be delegated to the Executive Vice President and Chief Operating Officer (or designee) to make further revisions or create new policies and standards as necessary be approved.

March 20, 2023